UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

v. Case No. 13-CR-00120-LA-WEC

PAUL CASE,

Defendant.

OBJECTIONS TO MAGISTRATE JUDGE WILLIAM E. CALLAHAN'S RECOMMENDATION AND ORDER (DOC. 33)

Paul Case, by counsel, submits his objections to Magistrate Judge William E. Callahan's Recommendation and Order pursuant to 28 U.S.C. §636(b)(1)(A), (B) and (C) and Federal Rules of Criminal Procedure 59(a) and (b)(2).

Introduction

In an affidavit supporting a search warrant for Case's home and computer, the affiant lied under oath: he concealed from the magistrate judge the fact that a data-mining computer program called RoundUp had been used to query the contents of Case's computer by claiming instead that the work was done by an "online covert employee" (OCE) of the FBI. The affidavit even gave the fictitious OCE a specific number as a fake identity. The government still has not disclosed what else the data-mining program did in or to Case's computer, or was capable of doing.

On the strength of that deliberately false statement—attributing the work of a computer program to a fictitious human being who supposedly worked for the

FBI and even had an operative number—Case moved the Magistrate Judge for an order granting a *Franks v. Delaware* hearing. The Magistrate Judge found that Case had not met his burden and denied the motion. Case herein objects to the Order of the Magistrate Judge.

While the defendant's motion was framed in accordance with traditional motions which seek a *Franks* hearing it also raised an issue of first impression which was not addressed by the Magistrate Judge.

On August 5, 2013, Reuters disclosed that this affiant probably was not alone: apparently the federal government systematically instructs agents to commit perjury in affidavits to conceal the existence and work of RoundUp and thus their true sources of information and activities. Attachment 1. No court has considered the impact of these false statements on *Franks v. Delaware* hearings. Consistent with the federal government manual dispensing such advice to deceive federal judges and others, counsel has discovered even more extensive lies by other federal agents in affidavits of child pornography cases in this district.

Case urges this Court to hold that, when the government acknowledges that deliberately false statements appear in affidavits by federal agents, the burden is on the government to explain why the agents lied and to convince a court not to strike from the affidavits the facts which were falsely attributed.

Argument

In accordance with the holding in *Franks v. Delaware* and its progeny the Magistrate Judge required that the movant bear the burden of proof to establish his

right to a *Franks* hearing. Case asserts both that he met that burden and, further, that on the novel facts here the government bears the burden and has from the beginning. No court has considered this issue as it did not arise prior to August 5, 2013. Specifically, the government must prove (1) whether it knew that the affiant in the search warrant affidavit had made a deliberate and intentional false statement concerning the source of his knowledge, (2) why the agent believed that he had the power and authority to assert this falsehood in a sworn statement to the Magistrate Judge and was immune to federal prosecution, and (3) that the false statement was not used to engage in what DOJ calls "parallel construction" search warrant applications—meaning investigations that start with known, unlawfully-obtained information as to which the agents then pretend to have obtained that information from a lawful source and recreate their investigation in parallel.[1]

Case asserts that where an agent has placed in a search warrant affidavit an admittedly false statement concerning the source of the evidence upon which the affiant relies, the government has the burden of proving that the agent had not engaged in a "parallel construction" process to conceal the unlawfulness of his acquisition of facts from the actual source.

The process of such deliberate falsity and concealment of the source of his facts by government agents was first disclosed in August 2013 and no court since that disclosure has discussed whether this falsity shifts the burden of proving its

[1]The Reuters news article attached as Attachment 1 to these Objections explains the term in some depth, along with context. In her Motion to Suppress Evidence Case's counsel asserted as grounds that the falsity in the search warrant affidavit was the product of a "parallel construction" investigative technique. Motion to Suppress at 1. Doc. 21. *See also* Affidavit of Robin Shellow in Support of *Franks* Motion paragraph 27 at 4. Doc. 21-1.

lawfulness to bar the defendant from a *Franks* hearing. It is that aspect of a *Franks* hearing that Case asks this Magistrate Judge to address in this objection.

Courts have allowed law enforcement agents to examine the contents of peer-to-peer networks to determine whether the defendant's computer has ever received or transmitted child pornography. However, these courts have limited the scope of these examinations to networks which are available to the public. In contrast, personal computer storage sites cannot be examined without a search warrant.

In this case, the affidavit in support of the search warrant stated that the peer-to-peer examination was conducted by an "online covert employee 5023." Paragraphs 25 and 27 of Brant A. Ungerer's affidavit in support of the issuance of the Case search warrant state:

> On November 24, 2012, around 2:11 a.m. Central Standard Time ("CST"), Online Covert Employee 5023 ("OCE-5023"), acting in an undercover capacity, conducted investigations into the sharing of child pornography files on the Ares P2P file sharing network. During this time, OCE-5023 identified a computer with the IP address 174.102.233.53 with at least seven files of investigative interest available for download.
>
> Between 02:11 a.m. CST on November 24, 2012, and 03:33 a.m. CST on November 25, 2012, OCE-5023 successfully completed downloads of five files containing child pornography from the computer at IP address 174.102.233.53, including the following three files: . .

United States' Response to Defendant's Motion to Suppress Evidence at 2-3, Doc. 23.

This statement in the affidavit was false and known to be false to the affiant. An "online covert employee" did not conduct the examination. There was no "online covert employee." The examination was performed by the RoundUp

computer program. This program and the manuals which describe the nature and extent of its examinations is available only to law enforcement officers.[2]

Precisely the same falsity appeared in the search warrant affidavit executed by F.B.I Special Agent Brett E. Banner in the case of Jeffrey Feldman, Case 2:13-mj-00421-WEC, Doc. 1 at page 4, pending before the Honorable Aaron

[2] On June 7, 2013, F.B.I. task force officer Ungerer executed a search warrant affidavit [Attachment 2] in 13-M-491 before the Honorable William E. Callahan, United States Magistrate Judge, Eastern District of Wisconsin, in which he again relied on online-covert-employee and stated in paragraph 7 at page 5,

> Between November 8, 2012 and March 29, 2013, **OCE-5023 (Online Covert Employee), acting in an undercover capacity, was conducting investigations into the sharing of child pornography files on the Ares P2P file sharing network.** Between these dates, OCE-5023 identified a computer with the IP address 75.129.148.54 sharing between 8 and 39 files of investigative interest available for download. Between the above dates OCE-5023 conducted four undercover sessions in an attempt to download the files of interest that the computer with the IP address 75.129.148.54 had available. OCE-5023 was only able to receive completed downloads from the computer at IP address 75.129.148.54 during three of the sessions. (emphasis added)

In paragraph 9 of the affidavit Ungerer stated,

> Between November 25, 2012, and March 29, 2013, during three separate undercover sessions, OCE-5023 successfully completed downloads of eleven files that were determined to be child pornography from the computer at IP address 75.129.148.54. The following are three of the files downloaded from the computer at IP address 75.129.148.54 by OCE-5023.

The government has not disclosed to defense counsel that OCE-5023 is not a person but a computer program.

On January 31, 2014, F.B.I. Special Agent Heather Wright in *United States v. Raul Gonzalez Sanchez*, Case No. 14-809u(NJ) filed a sworn criminal complaint before the Honorable Nancy Joseph, United States Magistrate Judge, Eastern District of Wisconsin, which also described the source of her information as an online-covert-employee (OCE) 5023 who 'continually conducts investigations into the sharing of child pornography files…" The affidavit in the following paragraphs outlines the investigations and findings of OCE-5023. Attachment 3.

The government has not disclosed to defense counsel that OCE-5023 is not a person but a computer program.

Goodstein, Magistrate Judge, Eastern District of Wisconsin.[3] In that case, as in the case *sub judice*, the purpose of the false statement was to conceal the agent's use of RoundUp. The affidavit stated in paragraphs 7 and 8,

PROBABLE CAUSE

> 7. Between June 10, 2012 and July 24, 2012, an FBI Online Covert law enforcement agent (hereinafter "OCE 4583"), while connected to the Internet in an online undercover capacity, conducted numerous online investigations to identify those individuals possessing and sharing child pornography using the eDonkey2000 (eD2K) and Kademlia (KAD) peer-to-peer (P2P) networks. OCE 4583 utilized a P2P file sharing program, which scans both networks simultaneously and has been enhanced to ensure that downloads occur only from a single selected source.
>
> 8. During those investigations, OCE 4583 searched for suspected child pornography files and identified IP address 65.30.43.173 on the KAD network which had suspected child pornography files available for distribution. Specifically, IP address 65.30.43.173 responded to OCE 4583's queries for the following suspected child pornography Shal hash values (also utilized by the KAD network) as outlined below:

Counsel has examined other search warrant affidavits in child pornography prosecutions in this district. Although they describe the affiant using computers to locate child pornography, they do not mention the RoundUp program nor falsely state that an online covert employee participated in the search and analysis.

The government claims that its misrepresentation and concealment of its use of the RoundUp program does not give rise to Fourth Amendment issues as the RoundUp program only identifies and downloads data on peer-to-peer networks and courts have held that since the public can access these networks, the defendant's privacy has not been invaded. Although only one opinion, *United States v. Bashear*, 2013 U.S. District Lexis 163865 (Nov. 18, 2013) has considered

[3] Undersign counsel also represents Jeffrey Feldman.

the government's use of RoundUp. The Court denied the defendant's motion for a Rule 17 subpoena for RoundUp's source codes on the grounds of relevancy.[4]

If the only data included in the search warrant affidavit was obtained from peer-to-peer networks, the agent would have no motivation to conceal his reliance on RoundUp. If RoundUp was programmed, either by its designers or modified by the agent, to access storage on Case's computer, or to insert data into this storage, the concealment of RoundUp's use was necessary to the agent's case and to Case's prosecution for child pornography offenses.

The agent's concealment that the RoundUp program was used to identify child pornography on the defendant's computer appears to be an instance of "parallel construction."

---

[4] The Court in *Bashear* wrote,

> The source code for the for the RoundUp program is not relevant because investigating the use of a peer-to-peer file sharing program does not violate the Fourth Amendment's protection against unreasonable searches.... Numerous cases have held that there is no reasonable expectation of privacy in files made available to the public through peer-to-peer file sharing programs. See, *e.g.*, *United States v. Stults*, 575 F.3d 834, 842-43 (8th Cir. 2009); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008).

United States v. Brashear, 2013 U.S. District Lexis 163865, 1-2 (Nov. 18, 2013).

> The investigation of a file sharing program does not involve any physical trespass onto a constitutionally protected area. Trooper Powell did not physically enter Brashear's home or access his computer. Instead, Trooper Powell simply used a program that identified child pornography available on a public peer-to-peer file sharing program. This investigation involves "the transmission of electronic signals without trespass" and does not implicate Brashear's Fourth Amendment rights under *Jones*.

Ibid. at 9-10.

The government in its Response to Defendant's Motion to Suppress Evidence offered no reason for the false statements in the search warrant affidavit, nor any discussion of the prosecutor's knowledge of this falsity. It is fair for this Court to conclude that there was a reason why the use of RoundUp was concealed by this falsity and why the affiant was willing to risk prosecution for the falsity, 18 U.S.C. §1001 or perjury. 18 U.S.C. §1621(1)[5] Counsel *infra* has shown that the tagging supplement to RoundUp actually inserts data in a suspect's computer and does so in such a way that the suspect will not know that tags have been placed in his computer's storage.

In recent months the government has acknowledged that its agents have used comparable subterfuges and federal agents are ordered to conceal such use in affidavits and from government and defense counsel and the courts. Wikipedia defines "parallel construction" as follows:

> Parallel construction is a police process of building a parallel - or separate - evidentiary basis for a criminal investigation which otherwise would rely upon evidence or tips received either from a confidential source or that might fall under the category of fruit of the poison tree.

The issue is thus raised whether the RoundUp program, as used in this case, limited its data gathering activities only to the peer-to-peer networks examinations which have been authorized by courts or whether RoundUp examined, analyzed

---

[5] "Wes Brot ich ess, des Lied ich sing." (Whose bread I eat, his song I sing.) -- Middle High German proverb.

In a prosecution for a violation of 18 U.S.C. 1001, the defendant could claim that the false statement was not material and hope that the jury would agree. *United States v. Lupton*, 620 F.3d 790 7th Cir. 2010). The probability of prosecution under that statute in this district is low as the government has claimed that the falsity is not material. United States' Sur-Reply Brief at 3. Doc. 31.

and downloaded or inserted other data which law enforcement agents are barred from doing.

RoundUp was designed under a Department of Justice grant by Professors in the Department of Computer Science at the University of Massachusetts Amherst and Georgetown University. After an extensive analysis of data acquired by law enforcement from peer-to-peer networks using RoundUp, these designers concluded that RoundUp had to be supplemented by a tagging program in which the investigating agent would insert a unique tag into the storage system of the suspect's computer. This tag would then be identified by the investigator after the suspect's computer was seized pursuant to a search warrant. The designers described their modification of the RoundUp protocol as follows:

> For this work, we built a system to gather evidence of possession of child pornography on a p2p [peer-to-peer] network. It is in use by law enforcement in all 50 U.S. states, specifically trained to use the software, who then provided us with data for almost a full year. To date, the system and its data have been used to obtain tens of thousands of search warrants. We characterize these measurements in order to motivate our tagging techniques. In contrast with methods used today, if our tags were found on a machine during a forensic exam, it would be strong evidence that the machine corresponds to observations of a peer made over the network. Unlike statistical characterization methods, our method has very strong privacy properties: the results can be recovered by investigators only after a search warrant is obtained from a judge. Tags observed by third parties are meaningless. Our careful analysis demonstrates that false positive probabilities can be driven to near zero. The tradeoff is the challenge to make sure tags are retained by the target, to be later discovered during an examination.
>
> * * *
>
> Our interest lies in effectively identifying the correct end system. In particular, can investigators strongly link network measurements with user behavior and intent? Our goals are twofold: First, we evaluate the quality of the procedures currently used to perform these measurements in Section 3. Thus, our second goal is to improve the quality of evidence and the range of tools available to investigators. In particular, we propose the use of tagging. The general mechanism of tagging is to insert bit patterns that are unique to each observation, which we call tags, into stable storage media belonging to a suspect during the course of the network-based investigation. These tags can later be recovered from the storage media following a legal seizure, not unlike marked bills might be

> recovered after an undercover transaction involving stolen property or illegal drugs. The tags can then be used to both link the observations with the media, and to show a pattern of behavior, and thus intent, on the part of the suspect.
>
> * * *
>
> We propose the tagging of remote machines by investigators, to leave a record of an observation on the remote machine for later recovery during warranted search.
>
> * * *
>
> Second, when directly connecting to a remote machine during an investigation, investigators use an appropriate vector to tag the machine. Tags are selected in such a way that their meaning is not obvious and to minimize the likelihood of collision. The investigator records the tags used to so that they can be validated when recovered.
>
> * * *
>
> For tagging to be practicable and of maximum value, several conditions must hold. First, a machine under investigation must be able to receive data from a remote source. Second, that data must be stored in a fashion that can be retrieved by investigators if the machine is physically seized. Third, investigators must be able to manipulate this data in such a way that it is specific to a single investigation — re-using tags dilutes or nullifies their evidentiary value, violating the assumptions we make in our security analysis. The information will only be recovered when legal authorization by means of a search warrant so allows. Here, we discuss the general manner by which such opportunities.

Efficient Tagging of Remote Peers During Child Pornography Investigations, Marc Liberatore, Brian Neil Levine, Clay Shields, Brian Lynn, Dept. of Computer Science, Univ. of Massachusetts Amherst, Dept. of Computer Science, Georgetown Univ. at 1-2, 3, 6, 11 https://web.cs.umass.edu/publication/docs/2012/UM-CS-2012-035.pdf

The designers of RoundUp estimated in a 2013 article, *Measurement and Analysis of Child Pornography Trafficking on P2P Networks*, that law enforcement in the United States used RoundUp in the preparation of approximately 150 search warrant affidavits per month. Case 2:13-cr-00155-LA-AEG, Exhibit 9 at page 3. "The data in this study formed the basis of 2,227 search warrant affidavits." *Ibid*. at page 1, footnote 3.

Courts have upheld the constitutionality of examining and analyzing the data on peer-to-peer networks on the grounds that communications with these networks by suspects are not intended to be private. The defendant asserts that it

is quite another matter for an agent to surreptitiously use this tagging supplement to RoundUp to insert identifying tags directly into the storage spaces of a suspect's computer.[6]

As an analogy: Suppose a DEA agent suspects someone of being a large purchaser of drugs. Using the approach described by designers of RoundUp and its tagging supplement, the agent breaks into the suspect's home and searches for money and then substitutes marked bills for the currency he finds. When the drugs are purchased, the agents arrest and search the seller for the marked bills and then get a search warrant for drugs at the purchaser's home concealing from the prosecutor, defense counsel and the Magistrate Judge that the agent had placed the marked bills in the purchaser's home and falsely representing that he received the incriminating information concerning the location of the drugs from a confidential informant.

---

[6] Even the designers of RoundUp and its supplementary tagging protocol are uncertain of the legality of its use on remote computers:

> Another relevant ruling for computer scientists is *Kyllo v. U.S.*, 533 U.S. 27 (2001), where the court ruled that using a technology that is not in general public use" to gather evidence pre-warrant is a violation of a person's expectation of privacy. This exact phrasing is important: source code available publicly on a researcher's web site is not general public use. With regard to digital forensics, this has been interpreted by investigators to mean that tools can only use information provided by normal operation of the system being investigated. Recent cases have supported this view, including *U.S. v. Borowy*, 595 F.3d 1045 (9th Cir. 2010) and *U.S. v. Gabel*, 2010 WL 3927697, but the exact extent to which can investigators can exploit a network protocol to gather information remotely is unsettled law.

Effective Digital Forensics Research is Investigator-Centric, Robert J. Walls Brian Neil Levine, Marc Liberatore Clay Shieldsy, Dept. of Computer Science, University of Amherst, MA, Dept. of Computer Science, Georgetown University, Washington, D.C. at 3.
https://www.usenix.org/legacy/events/hotsec11/tech/final_files/Walls.pdf

Conclusion

While a false statement in a search warrant concerning the source of the affiant's evidence does not by itself provide the basis for a *Franks v. Delaware* hearing, it does however require the prosecution to establish that the concealment of its use of RoundUp in the agent's search warrant affidavit was not an implementation of parallel construction designed to conceal from the prosecution, defense counsel and the Magistrate Judge that the agent acquired data that he had no right to examine or insert.

If the RoundUp data included in the affidavit for the Case's search warrant was obtained in violation of law then the defendant is entitled to a *Franks v. Delaware* hearing and to a judicial determination of whether probable cause remains after the unlawfully acquired data is excluded.

Dated this 6th day of February, 2014.

Respectfully Submitted,

__s/Robin Shellow_____
Robin Shellow, #1006052
The Shellow Group
324 West Vine Street
Milwaukee, Wisconsin 53212
Tel.: 414-263-4488
tsg@theshellowgroup.com

James M. Shellow, #1006070
Shellow & Shellow, S.C.
324 West Vine Street
Milwaukee, Wisconsin 53212
jamesgilda@aol.com

Attorneys for Paul Case